United Nations A/HRC/31/NGO/49

General Assembly

Distr.: General
17 February 2016

English only

Human Rights Council
Thirty-first session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Privacy International, a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[08 February 2016]

* This written statement is issued, unedited, in the language(s) received from the submitting non-governmental organization(s).

GE.16-02318(E)

Please recycle

Concerns about the right to privacy in new surveillance laws

In recent years, the UN has paid significantly increased attention to modern forms of communications surveillance and their effects on the right to privacy and other human rights.

In its 2015 resolution on the right to privacy in the digital age, the Human Rights Council expressed deep concerns at the negative impact that surveillance may have on the exercise and enjoyment of human rights, most notably the right to privacy.[1] By establishing the UN Special Rapporteur on the right to privacy, the Council filled a significant gap in the international human rights protection system.

The Universal Periodic Review in 2015 has already witnessed increased attention on issues of privacy in the digital age: some governments made recommendations related to modern communications surveillance law during the reviews of Australia, Austria, Belarus, Kenya, Sweden, Turkey, and the USA.[2] These recommendations constitute an important sign that the right to privacy is finally receiving due attention within the UPR framework.

Meanwhile, while considering state parties' implementation of the International Covenant on Civil and Political Rights (ICCPR) in 2015, the Human Rights Committee expressed serious concerns about surveillance powers in Canada, France, the Former Yugoslav Republic of Macedonia, the Republic of Korea, and the United Kingdom.[3] In doing so, the Committee reaffirmed some very important elements of its interpretation of Article 17 of the ICCPR as it applies to modern communications surveillance. Most notably, the Committee held that the right to privacy needs to be respected regardless of the nationality or location of individuals whose communications are under surveillance; that states should establish robust oversight systems for surveillance and intelligence-sharing activities; and that states must ensure there is judicial involvement in the authorisation of such measures in all cases, including in relation to communications data.

This attention on communication surveillance and its implications for the right to privacy has undoubtedly resulted in the recognition of the need to review and reform laws, and to make the work of the intelligence and security agencies more open to independent scrutiny, including parliamentary oversight. This was reflected in the 2014 UN General Assembly resolution on the right to privacy in the digital age, which called on all states to "review their procedures, practices and legislation regarding the surveillance of communications [...] with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law".[4]

Regretfully, however, many governments have been adopting laws or proposing legislation that increase their intrusive powers of surveillance or seek to legalise post facto the privacy invasive practices of their security services in ways that fall short of applicable international human rights standards.

China introduced new anti-terrorism legislation in December 2015. While the new law does not go as far as requesting companies to hand over encryption keys, it does require companies hand over technical information and help with decryption.[5]

In France two new surveillance laws have been debated and adopted in less than twelve months.[6] These laws, as well as the current state of emergency, impose excessive and disproportionate restrictions on the right to privacy and other

---

1 UN doc. A/HRC/RES/28/16, 1 April 2015.

2 See Australia (UN doc. A/HRC/WG/6.23/L.11), Austria (UN doc. A/HRC/31/12), Belarus (UN doc. A/HRC/30/3), Kenya (UN Doc. A/HRC/29/10), Sweden (A/HRC/29/13), Turkey (UN doc. A/HRC/29/15), United States (UN doc. A/HRC/30/12.)

3 See Human Rights Committee's concluding observations on periodic reports of Canada (UN doc. CCPR/C/CAN/CO/6), France (UN doc. CCPR/C/FRA/CO/5), the Former Yugoslav Republic of Macedonia (UN doc. CCPR/C/MKD/CO/3), the Republic of Korea (UN doc. CCPR/C/KOR/CO/4), and the United Kingdom (UN doc. CCPR/C/GBR/CO/7.)

4 UN doc. A/RES/69/166, 10 February 2015.

5 See http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism-law-that-critics-fear-may-overreach.html

6 The Intelligence Law n.2015-912 of 24 July 2015 (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&ca) and the International Surveillance law n° 2015-1556 of 30 November 2015 (http://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte).

fundamental freedoms, as noted by the Human Rights Committee in July 2015[7] and by five UN Special Rapporteurs in January 2016.[8]

In Kenya, the Security Law (Amendment) Act 2014 expands the surveillance powers of the intelligence services, while at the same time weakening the judicial authorisation procedure.[9] In January 2016, Poland fast tracked a reform of its surveillance law further expanding the powers of the surveillance agencies in ways that infringe Polish obligations under the ICCPR.[10]

Meanwhile draft bills on communications surveillance are being debated in a number of countries. While not yet adopted, the indication is that governments are seeking to expand their surveillance beyond what is necessary and proportionate under international human rights standards.

In the Netherlands, the draft Law on Intelligence and Security Services 2015 seeks to introduce provisions that raise serious concerns about compliance with international human rights standards, including notably extending the power of intelligence and security services to conduct mass surveillance. The bill also includes provisions aimed at weakening encryption and at allowing states to hack into computers and devices.

In Pakistan, the government introduced the Prevention of Electronic Crime Bill which contains a range of provisions that, if adopted, would have affect the right to privacy and freedom of expression, particularly by requiring service providers to retain telephone and e-mail communications data for a minimum of one year and by allowing for unchecked intelligence sharing with foreign governments.[11] Following concerns expressed by national and international non-governmental organisations[12] and the UN Special Rapporteur on freedom of expression[13], the Bill has been held for further consultation.

In Switzerland, a new law to regulate surveillance, the Nachrichtendienstgesetz (NDG), introduces powers to intercept communications running through internet cables that pass through Switzerland; and infiltrate computer networks through government hacking.[14] The law is currently the subject of a referendum scheduled to take place in June, an initiative spearheaded by a range of political parties and activists concerned about the scope of the surveillance powers contained in the law.[15]

In the United Kingdom, the government introduced the draft Investigatory Powers Bill on 4 November 2015 with the stated aim to overhaul existing surveillance legislation and set a"gold standard" for governments around the world.[16] The current draft falls significantly short of this goal. Instead, the IP Bill seeks to legalise and expand the already overly broad powers of the UK intelligence and police services. Three UN Special Rapporteurs have already expressed concerns at some of its provisions in written evidence to the Parliamentary Joint Committee on the IP Bill.[17]

Often framed as responses to terrorist threats, these surveillance laws and proposals support an approach to security and counter-terrorism that treats the privacy of individuals as an impediment to the pursuit of vaguely defined national

---

7 See Human Rights Committee, Concluding observations on France.

8 See http://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=16961&LangID=F

9 See http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf

10 See Amnesty International, Poland: New surveillance law a major blow to human rights, 29 January 2016, https://www.amnesty.org/en/documents/eur37/3357/2016/en/?refresh

11 See https://www.privacyinternational.org/sites/default/files/Prevention-of-Electronic-Crimes-Bill-2015%20Legal%20Analysis_0.pdf

12 See https://www.privacyinternational.org/node/682

13 See http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16879&LangID=E

14 See http://grundrechte.ch/2015/6597.pdf

15 See http://grundrechte.ch/CMS//francais.html and https://theintercept.com/2016/01/25/how-a-small-company-in-switzerland-is-fighting-a-surveillance-law-and-winning/

16 See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

17 See http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26353.html

security aims - wrongly arguing that we can have either security or privacy, but not both. This approach risks widening the gap between States' legal and technological capabilities and applicable human rights standards.

As affirmed by the UN General Assembly and Human Rights Council, international human rights law provides a clear and universal framework to respect and protect the right to privacy, including in the context of modern communications surveillance. The High Commissioner for Human Rights, UN special rapporteurs and the Human Rights Committee have already demonstrated how existing standards can be interpreted to address some of the challenges posed by modern communications surveillance. In a similar way, the European Court on Human Rights and the Court of Justice of the European Union have delivered judgments that clarify the scope of application of the right to privacy and the limits existing human rights standards impose on states' communications surveillance powers.[18] And civil society organisations have developed, based on the existing standards and jurisprudence, the International Principles on the Application of Human Rights to Communications Surveillance.[19]

To close the gap between existing human rights standards and surveillance laws and practices that infringe upon the right to privacy, Privacy International believes that UN human rights experts and the Council need to continue to systematically monitor and assess states' laws, policies and practices, report on violations and develop specific recommendations.

---

18 See in particular European Court on Human Rights, Grand Chamber judgment Zakharov v. Russia, 4 December 2015; Szabó and Vissy v. Hungary, 12 January 2016; and Court of Justice of the European Union, Grand Chamber judgment, Schrems v. Data Protection Commissioner, 6 October 2015.

19 See https://necessaryandproportionate.org